ABSTRACT

Methods and apparatuses are provided for generating blind digital signatures using curve-based cryptography techniques. One exemplary method includes establishing parameter data for use with signature generating logic that encrypts data based on a Jacobian of at least one curve. Here, the parameter data causes the signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to the curve. The method also includes receiving first data that is to be blindly signed, determining private key data and corresponding public key data using the signature generating logic, and generating second data by signing the first data with the private key data using the signature generating logic. The second data includes the corresponding blind digital signature. In other implementations, the method may also include having additional logic, for example, in one or more other devices, determine if the blind digital signature is valid.